UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/855,714	05/16/2001	Kazuaki Ebara	31869-171865	9422

26694   7590   05/02/2005

VENABLE LLP
P.O. BOX 34385
WASHINGTON, DC 20435-9998

EXAMINER
HOFFMAN, BRANDON S

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 05/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/855,714	EBARA, KAZUAKI
	Examiner	Art Unit	
	Brandon Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>09 March 2005</u>.
2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
   closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>1-19</u> is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) <u>1-19</u> is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.
10) ☒ The drawing(s) filed on <u>16 May 2001</u> is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a) ☐ All   b) ☐ Some * c) ☐ None of:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____.
   3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage
      application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
   Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1-19 are pending in this office action. Claims 16-19 are newly added.

2.   Applicant's arguments, filed March 9, 2005, have been considered and are

persuasive. However, a new ground of rejection is made.

Drawings

3.   The drawing objections are corrected.

Rejections

4.   The text of those sections of Title 35, U.S. Code not included in this action can

be found in a prior Office action.

Claim Rejections - 35 USC § 103

5.   <u>Claims 1-19</u> are rejected under 35 U.S.C. 103(a) as being unpatentable over

<u>Zoka</u> (U.S. Patent No. 6,591,249) in view of <u>Johnson</u> (U.S. Patent No. 6,529,885).

Regarding <u>claim 1</u>, <u>Zoka</u> teaches a biometric authentication system comprising a

first enterprise system, a second enterprise system, and a communication network

interconnecting the first enterprise system and the second enterprise system (fig. 5, ref.

num 24, 30, and 48), wherein:

The first enterprise system includes:

- A registration apparatus for acquiring a user's biometric information in advance of

  authentication, extracting features therefrom, and converting the features to

  template data (fig. 3),

- A first·authentication apparatus for acquiring the user's biometric information

  during authentication, extracting features therefrom, and converting the features

  to authentication data (fig. 2, ref. num 16), and

- A first database server apparatus for receiving the template data from the

  registration apparatus, storing and managing the template data, receiving the

  authentication data from the first authentication apparatus during authentication,

  comparing the authentication data with the template data, thereby authenticating

  the user (fig. 6 and 7); and

The second enterprise system includes:

- A second authentication apparatus for acquiring the user's biometric information,

  extracting features therefrom, and converting the features to authentication data

  (fig. 5 and col. 8, line 61 through col. 9, line 3).

Zoka does not teach a second database server apparatus for receiving the

authentication data from the second authentication apparatus, requesting corresponding

template data from the first database server apparatus, receiving the corresponding

template data from the first database server apparatus, comparing the authentication

data with the corresponding template data, thereby authenticating the user, and storing

and managing the received template data if the user is authenticated successfully.

Johnson teaches a second database server apparatus for receiving the

authentication data from the second authentication apparatus, requesting corresponding

template data from the first database server apparatus, receiving the corresponding

template data from the first database server apparatus, comparing the authentication

data with the corresponding template data, thereby authenticating the user, and storing

and managing the received template data if the user is authenticated successfully (fig.

2, col. 6, lines 31-49, and col. 12, line 27 through col. 14, line 19).

It would have been obvious to one or ordinary skill in the art, at the time the

invention was made, to combine the second database server apparatus receiving

authentication data from the second apparatus, requesting template data from the first

apparatus, comparing the received data with the generated data, and storing the

received template data, as taught by Johnson, with the system of Zoka. It would have

been obvious for such modifications because storing initial authentication information at

a source that a user trusts (the web buyer's home bank) provides user trust in online

systems. Also, only allowing non-critical data to be supplied to the web seller helps

prevent critical data (passwords, account information) from being transmitted across

open networks (see col. 14, lines 20-64 of Johnson).

Regarding claim 2, Zoka as modified by Johnson teaches wherein the second

database server apparatus sends the authentication data received from the second

authentication apparatus to the first database server apparatus, and the first database

server apparatus includes a one-to-many biometric identification unit that performs a

one-to-many comparison between the authentication data received from the second

database server apparatus and all of the template data stored and managed by the first

database server apparatus to find the template data corresponding to the authentication

data (see col. 9, lines 3-19 of Zoka).

Regarding claims 3, 6, and 10, Zoka as modified by Johnson teaches wherein

the first database server apparatus includes a billing unit that charges the second

enterprise system a fee when the second database server apparatus requests

corresponding template data and the first database server apparatus sends the

corresponding template data and personal information to the second database server

apparatus (see col. 13, lines 50-52 of Johnson).

Regarding claim 4, Zoka as modified by Johnson teaches wherein the second

database server apparatus sends the authentication data received from the second

authentication apparatus to the first database server apparatus when requesting the

corresponding template data, and the first database server apparatus includes a one-to-

many biometric identification unit that performs a one-to-many comparison between the

authentication data received from the second database server apparatus and all of the

template data stored and managed by the first database server apparatus to find the

template data corresponding to the authentication data (see col. 9, lines 3-19 of Zoka).

Regarding claim 5, Zoka as modified by Johnson teaches wherein:

- The first database server apparatus includes a first personal-information database storing personal information about the user (see col. 5, lines 40-46 of Zoka);

- When the first database server apparatus sends the corresponding template data to the second database server apparatus, the first database server apparatus also sends the personal information about the user to the second database server apparatus (see col. 9, lines 11-19 of Zoka); and

- The second database server apparatus includes a second personal-information database that stores and manages the personal information about the user received from the first database server apparatus (see col. 14, lines 5-19 of Johnson).

Regarding claim 7, Zoka teaches a biometric authentication system comprising a first enterprise system, a second enterprise system, and a communication network interconnecting the first enterprise system and the second enterprise system (fig. 5, ref. num 24, 30, and 48), wherein:

The first enterprise system includes:

- A registration apparatus for acquiring a user's biometric information in advance of authentication, extracting features therefrom, and converting the features to template data (fig. 3),

- A first authentication apparatus for acquiring the user's biometric information during authentication, extracting features therefrom, and converting the features to authentication data (fig. 2, ref. num 16), and

- A first database server apparatus for receiving the template data from the
  registration apparatus, storing and managing the template data, receiving the
  authentication data from the first authentication apparatus during authentication,
  comparing the authentication data with the template data, thereby authenticating
  the user, receiving authentication data from the second enterprise system, and
  returning corresponding template data to the second enterprise system if the
  corresponding template data is stored in the first database server apparatus (fig.
  6 and 7 and col. 9, lines 3-19); and

  The second enterprise system includes:

- A simplified registration apparatus for acquiring the user's biometric information
  during registration, extracting features therefrom, and converting the features to
  authentication data (col. 1, lines 7-16),

- A second authentication apparatus for acquiring the user's biometric information
  during authentication, extracting features therefrom, and converting the features
  to authentication data (fig. 5 and col. 8, line 61 through col. 9, line 3).

Zoka does not teach a second database server apparatus for receiving the
authentication data from the simplified registration apparatus and the second
authentication apparatus, sending the authentication data received from the simplified
registration apparatus to the first database server apparatus, receiving the
corresponding template data from the first database server apparatus, storing and
managing the received template data, and comparing the authentication data received

from the second authentication apparatus with the stored template data, thereby

authenticating the user.

Johnson teaches a second database server apparatus for receiving the

authentication data from the simplified registration apparatus and the second

authentication apparatus, sending the authentication data received from the simplified

registration apparatus to the first database server apparatus, receiving the

corresponding template data from the first database server apparatus, storing and

managing the received template data, and comparing the authentication data received

from the second authentication apparatus with the stored template data, thereby

authenticating the user (fig. 2, col. 6, lines 31-49, and col. 12, line 27 through col. 14,

line 19).

It would have been obvious to one or ordinary skill in the art, at the time the

invention was made, to combine the second database server apparatus receiving

authentication data from the second apparatus, requesting template data from the first

apparatus, comparing the received data with the generated data, and storing the

received template data, as taught by Johnson, with the system of Zoka. It would have

been obvious for such modifications because storing initial authentication information at

a source that a user trusts (the web buyer's home bank) provides user trust in online

systems. Also, only allowing non-critical data to be supplied to the web seller helps

prevent critical data (passwords, account information) from being transmitted across

open networks (see col. 14, lines 20-64 of Johnson).

Regarding claim 8, Zoka teaches a database server apparatus for use in a first

enterprise system that is linked by a communication network to a second enterprise

system (fig. 5, ref. num 24, 30, and 48), for receiving biometric template data and

biometric authentication data from the first enterprise system, storing and managing the

biometric template data (fig. 6 and 7), comparing the biometric authentication data with

the biometric template data, thereby authenticating users of the first enterprise system.

Zoka does not teach supplying the biometric template data on request to the

second enterprise system to enable users of the first enterprise system to become

registered with the second enterprise system.

Johnson teaches supplying the biometric template data on request to the second

enterprise system to enable users of the first enterprise system to become registered

with the second enterprise system (fig. 2, col. 6, lines 31-49, and col. 12, line 27 through

col. 14, line 19).

It would have been obvious to one or ordinary skill in the art, at the time the

invention was made, to combine supplying template data to the second apparatus upon

request to enable users of the first apparatus to become registered with the second

apparatus, as taught by Johnson, with the apparatus of Zoka. It would have been

obvious for such modifications because storing initial authentication information at a

source that a user trusts (the web buyer's home bank) provides user trust in online

systems. Also, only allowing non-critical data to be supplied to the web seller helps

prevent critical data (passwords, account information) from being transmitted across

open networks (see col. 14, lines 20-64 of Johnson).

Regarding claim 9, Zoka as modified by Johnson teaches comprising a one-to-

many biometric identification unit that performs a one-to-many comparison between

biometric authentication data received from the second enterprise system and the

biometric template stored and managed by the first database server apparatus to find

the biometric template data requested by the second enterprise system (see col. 9, lines

3-19 of Zoka).

Regarding claim 11, Zoka as modified by Johnson teaches comprising a

personal-information database storing personal information about the users of the first

enterprise system, the personal information being sent to the second enterprise system

together with the biometric template data requested by the second enterprise system

(see col. 5, lines 40-46 of Zoka).

Regarding claim 12, Zoka as modified by Johnson teaches wherein the database

server apparatus receives biometric authentication data from the second enterprise

system, compares the received biometric authentication data with the requested

biometric template data, and sends the requested biometric template data to the second

enterprise system only if the received biometric authentication data match the requested

biometric template data (see fig. 2, col. 6, lines 31-49, and col. 12, line 27 through col.

14, line 19 of Johnson).

Regarding <u>claim 13,</u> <u>Zoka</u> teaches a database server apparatus for use in a

second enterprise system that is linked by a communication network to a first enterprise

system (fig. 5, ref. num 24, 30, and 48), for receiving biometric authentication data from

the second enterprise system (col. 1, lines 7-16).

<u>Zoka</u> does not teach requesting corresponding biometric template data from the

first enterprise system, receiving the requested biometric template data from the first

enterprise system, storing and managing the received biometric template data, and

comparing the biometric authentication data with the stored biometric template data,

thereby authenticating users of the second enterprise system.

<u>Johnson</u> teaches requesting corresponding biometric template data from the first

enterprise system, receiving the requested biometric template data from the first

enterprise system, storing and managing the received biometric template data, and

comparing the biometric authentication data with the stored biometric template data,

thereby authenticating users of the second enterprise system (fig. 2, col. 6, lines 31-49,

and col. 12, line 27 through col. 14, line 19).

It would have been obvious to one or ordinary skill in the art, at the time the

invention was made, to combine requesting template data from the first apparatus,

storing the received template data, and comparing the received template data with the

produced data for authenticating the user, as taught by <u>Johnson</u>, with the apparatus of

<u>Zoka</u>. It would have been obvious for such modifications because storing initial

authentication information at a source that a user trusts (the web buyer's home bank)

provides user trust in online systems. Also, only allowing non-critical data to be

supplied to the web seller helps prevent critical data (passwords, account information)

from being transmitted across open networks (see col. 14, lines 20-64 of Johnson).

Regarding claim 14, Zoka as modified by Johnson teaches wherein the database

server apparatus sends the biometric authentication data received from the second

enterprise system to the first enterprise system when requesting the corresponding

biometric template data from the first enterprise system (see col. 12, lines 42-56 of

Johnson).

Regarding claim 15, Zoka as modified by Johnson teaches comprising a

personal-information database for storing personal information about the users of the

second enterprise system; the personal information being received from the first

enterprise system together with the requested biometric template data (see col. 9, lines

11-19 of Zoka).

Regarding claims 16-19, Zoka as modified by Johnson teaches wherein the first

enterprise system receives the user's biometric information from the second enterprise

system, uses the user's biometric information to retrieve the template data, and sends

the retrieved template data to the second information system; and wherein the second

enterprise information system performs authentication using the retrieved template data

sent by the first enterprise system (see fig. 2, col. 6, lines 31-49, and col. 12, line 27

through col. 14, line 19 of Johnson).

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Brandon S. Hoffman whose telephone number is 571-

272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for

the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

BH

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100